PTO/SB/21 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/650,712
Filing Date	8/29/2000
First Named Inventor	Rico Mariani
Group Art Unit	2131
Examiner Name	SHIN HON CHEN
Attorney Docket Number	MS1-579US

Total Number of Pages in This Submission

ENCLOSURES (check all that apply)

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☒ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Documents
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) *(please identify below):*

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual Name	Kayla D. Brant, Reg. No. 46575
Signature	Kayla D Brant
Date	6/21/05

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Carly Taylor	
Signature	Carly Taylor	Date 6/21/05

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/650,712
Filing Date 08/29/2000
Inventorship..... Mariani, Rico
Applicant ..... Microsoft Corporation
Group Art Unit 2131
Examiner .....Chen, Shin Hon
Attorney's Docket No. MS1-0579US
Title: Systems and Methods for Limiting Access to Potentially Dangerous Code

APPEAL BRIEF

To: Board of Patent Appeals and Interferences
Alexandria, VA 22313-1450

From: Kayla D. Brant Tel. 509-324-9256 ext. 242
Fax 509-323-8979
Customer # 22801

Pursuant to 37 C.F.R. § 41.37 and 37 C.F.R. § 1.136(a), Applicant hereby submits a supplemental appeal brief for application 09/650,712 within four months from the filing date of the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

TABLE OF CONTENTS

(1) Real Party in Interest

The real party in interest is the Microsoft Corporation, the assignee of all right and title to the subject invention.

(2) Related Appeals and Interferences

There are no related appeals or interferences.

(3) Status of Claims

Claims 1-10, 17-23, 27, 28, 30-32, and 34 are pending in this Application, and are set forth in the Appendix of Appealed Claims on page 20. Claims 1-10, 17-23, 27, 28, 30-32, and 34 stand rejected. Claims 1-35 were originally filed in the Application. Claims 11-16, 24-26, 29, 33, and 35 were cancelled, and claims 7-10, 17, 27, 30, and 32 were amended in an amendment filed July 29, 2004. No claims have been allowed.

Claims 1-10, 17-23, 27, 28, 30-32, and 34 are subject to this appeal and stand rejected as set forth in a Final Office Action dated January 11, 2005. Specifically:

Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are rejected under 35 U.S.C. § 102(e) as being clearly anticipated by U.S. Patent 6,499,109 issued to Balasubramaniam et al. (hereinafter, "Bal") (*1/11/2005 Office Action* p.2).

Claim 3 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of U.S. Patent No. 6,499,105 issued to Yoshiura (hereinafter, "Yoshiura") and further in view of U.S. Patent No. 6,058,482 issued to Liu (hereinafter, "Liu") (*1/11/2005 Office Action* p.5).

Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal

in view of Yoshiura (*1/11/2005 Office Action* p.6).

Claim 6 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of U.S. Patent No. 6,615,088 issued to Myer et al. (hereinafter, "Myer") (*1/11/2005 Office Action* p.6).

Claims 19, 32, and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of Renaud (*1/11/2005 Office Action* p.8).

Claims 27, 28, 30, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of Liu (*1/11/2005 Office Action* p.9).

(4) Status of Amendments

A rejection to claims 1-35 was issued on May 6, 2004 whereupon Applicant responded to address the Examiner's rationale for the rejection and to cancel claims 11-16, 24-26, 29, 33, and 35 and amend claim 7-10, 17, 27, 30, and 32. The claim amendments were entered, and subsequently, a final rejection was issued on January 11, 2005. A Notice of Appeal was filed on March 18, 2005. No amendments have been filed subsequent to the Examiner's final rejection dated January 11, 2005.

(5) Summary of Claimed Subject Matter

Following is a concise explanation of each independent claim 1, 7, 17, 27, and 32 involved in the Appeal which includes specification references and exemplary drawing reference characters. As explained, the independent claims are not limited solely to the elements identified by the reference characters.

The claimed subject matter is directed to authenticating a digital signature associated with a web page prior to executing a least a portion of the web page. Specifically:

Claim 1 includes associating a digital signature (226) with a web page (212); and delivering the web page (212) to an electronic device (204).

Claim 7 describes receiving a web page (212') having a digital signature (226') that can be used to identify a source of the web page. (*Application, pg. 14, lines 11-12; Figure 3, block 308.*) The web page (212') contains executable script (216') that, when executed invokes a control object (218'). (*Application, pg. 12, lines 5-7.*) The web page is displayed and the control object invoked only if the source of the web page is determined to be authentic based on the digital signature associated with the web page. (*Application, pg. 15, lines 14-19.*)

Claim 17 describes a computer system (204) that includes a web browser (230) for accessing a web page (212') that has an associated digital signature (226'), a processor (227) configured to execute script (216') that may be contained in the web page (212'), an executable control object (218') that may be invoked by the script in the web page, and a confirmation module (220') configured to authenticate the digital signature to determine, based on authenticity of the digital signature, whether the control object should be invoked. (*Application, pg. 13, lines 8-18; Figure 2, Client Computer 204.*)

Claim 27 describes a web browser (230) that determines if a received web page (212') contains instructions to invoke a control object (218') and determines if the web page has an associated digital signature (226'). If the web page has an associated digital signature, the browser authenticates the web page using the digital signature, and invokes the control object if the source of the web page is authenticated. (*Application, pg. 14, line 11-pg. 15, line 19.*)

Claim 32 describes a control object (218') that authenticates a web page (212') that invokes the control object. The authentication is performed based on a digital signature (226') associated with the web page. A data-handling task is performed on the computer if the web page is determined to be authentic. (*Application, pg. 13, lines 1-7.*)

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,499,109 issued to Balasubramaniam et al. (hereinafter, "Bal") (*1/11/2005 Office Action* p.2).

Claim 3 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of U.S. Patent No. 6,499,105 issued to Yoshiura (hereinafter, "Yoshiura") and further in view of U.S. Patent No. 6,058,482 issued to Liu (hereinafter, "Liu") (*1/11/2005 Office Action* p.5).

Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of Yoshiura (*1/11/2005 Office Action* p.6).

Claim 6 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of U.S. Patent No. 6,615,088 issued to Myer et al. (hereinafter, "Myer") (*1/11/2005 Office Action* p.6).

Claims 19, 32, and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of Renaud (*1/11/2005 Office Action* p.8).

Claims 27, 28, 30, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal in view of Liu (*1/11/2005 Office Action* p.9).

(7) Argument

Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are not anticipated by Bal.

Claims1, 2, and 5

Bal describes verifying the source of software downloaded from a remote site to a client computer over a computer network before the software can be executed on the client computer. (Bal, Abstract.) Specifically, Bal describes a computer-executable program code that first determines the URL to which a browser running on the client computer is pointed and enables the downloaded software program only if the URL to which the browser is pointed is an authorized URL. (Bal, Summary.) Bal is akin to a scenario Applicant describes in the Background section that is improved with the claimed technique.

Independent claim 1 recites:

> A method, comprising:
>
> associating a digital signature with a web page; and
>
> delivering the web page to an electronic device capable of authenticating the digital signature and executing at least a portion of the web page after the digital signature is authenticated.

In contrast to the method of claim 1, Bal describes examining a URL to which a browser is pointed to determine whether or not to allow execution of downloaded software. Bal does not describe "associating a ***digital signature with a web page,***" nor does Bal describe "delivering the web page to an electronic device capable of ***authenticating the digital signature*** and executing at least a portion of the web page after the digital signature is authenticated," as claimed. The Office cites Bal, column 7, lines 32-38 as describing "associating a digital signature with a web page." (*1/11/2005 Office Action* p.2) However, the cited portion of Bal (column 7, lines 32-38) states, "initiating the downloading of a web page on the browser window on the client computer based on the URL, wherein the web page has associated therewith a control software program with a corresponding digital signature; verifying the control software program using the digital signature." This portion of Bal clearly states that a digital signature is associated with the control software program – ***not*** with the web page, as found in

claim 1. Furthermore, Bal, claim 1, of which the cited language is a portion, goes on to recite, "querying the browser program to determine the URL to which the browser program is pointed; determining whether the URL to which the browser program is pointed is authorized; executing the control software program if it is determined that *the URL to which the browser program is pointed* is authorized." Bal describes executing downloaded software based on authentication of a URL to which a browser program is pointed. Bal does not describe executing at least a portion of the web page after the digital signature is authenticated, where the digital signature is associated with the web page, as recited in claim 1. Accordingly, claim 1 is allowable over Bal.

Claims 2 and 5 are allowable by virtue of their dependency on claim 1.

Claims 7-10

Independent claim 7 recites:

> A method, comprising:
>
> receiving a web page from a server, the web page containing executable script that, when executed, invokes a control object, **the web page having a digital signature that can be used to identify a source of the web page;**
>
> determining whether the source of the web page is authentic **via the digital signature**; and
>
> in an event that the source of the web page is authentic, displaying the web page and invoking the control object

In contrast to claim 7, Bal describes verifying a URL associated with a web page, and executing a control software program only after verification of the URL. (Bal, column 7, lines 26-51 – claim 1.) As stated above with reference to claim 1, Bal does not describe "a web page having a digital signature that can be used to identify a source of the web page," as claimed. Accordingly, claim 7 is allowable over Bal.

Claims 8-10 are allowable by virtue of their dependency on claim 7.

Claims 17, 18, and 20-23

Independent claim 17 recites:

> A system, comprising:
>
> a web browser configured to access **a web page having a digital signature;**
>
> a processor configured to execute script contained in the web page;
>
> **an executable control object that may be invoked by the script in the web page** and is executable on the processor; and
>
> a confirmation module configured to **authenticate the digital signature to determine** based on authenticity of the digital signature, **whether the control object should be invoked.**

In contrast to claim 7, Bal describes authenticating a digital signature associated with a control software program and verifying a URL associated with a

web page, to determine whether to execute the control software program. (Bal, column 7, lines 26-51 – claim 1.) As stated above with reference to claim 1, Bal does not describe "a web page having a digital signature," as claimed. Furthermore, Bal does not describe authenticating the **digital signature** associated with the web page to determine whether the control object should be invoked. Rather, Bal describes verifying a **URL** associated with the web page to determine whether a control object should be invoked. Accordingly, claim 17 is allowable over Bal.

Claims 18 and 20-23 are allowable by virtue of their dependency on claim 17.

Claim 3 is not taught or suggested by the combination of Bal, Yoshiura, and Liu.

Claim 3

Dependent claim 3 recites:

> The method as recited in claim 1, further comprising:
>
> determining if the web page includes code to invoke a control object; and
>
> deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

As described above, Bal describes determining a URL to which a browser running on a client computer is pointed and enabling a downloaded software program only if the URL to which the browser is pointed is an authorized URL. (Bal, Summary.) Bal does not describe "associating a digital signature with a web page," as recited in claim 1, from which claim 3 depends. Furthermore, Bal does not describe, nor does the Office contend that Bal describes, "determining if the web page includes code to invoke a control object; and deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object," as recited in claim 3.

Yoshiura describes a method for identifying a purchaser who purchased content from which an illegal copy was produced. (Yoshiura, Abstract.) Liu describes a server process for identifying a particular keyword in a web page, and then modifying the web page to enable secure download of executable code associated with the web page. Both Yoshiura and Liu fail to add any teaching to Bal regarding the features recited in claim 1. Namely, the combination of Bal, Yoshiura, and Liu fails to teach "associating a ***digital signature with a web page***" and "executing at least a portion of the web page after ***the digital signature*** is authenticated," as recited in claim 1.

Additionally, there is no suggestion to combine the teachings of Bal and Yoshiura. Yoshiura describes a method for identifying a purchaser who purchased content from which an illegal copy was produced. (Yoshiura, Abstract.) There is nothing in Yoshiura to suggest that identifying a purchaser of content has anything to do with authenticating access to executable code that may be invoked from a web page.

Furthermore, while Liu may disclose determining whether or not a web page includes code to invoke a control object, Liu does not teach or suggest using that information to determine whether or not to generate and associate a digital signature with the web page. Rather, Liu discloses using that information to determine whether or not to modify the web page to enable secure download of specific portions of executable code associated with the web page over a network. Liu describes processing that is performed in association with a web page that includes executable code that will need to be downloaded in order to be run. Liu does not suggest performing such processing in association with a web page that includes code that invokes a control object that may have already been downloaded. Accordingly, claim 3 is allowable over Bal in view of Yoshiura and further in view of Liu.

Claim 4 is not taught or suggested by the combination of Bal and Yoshiura.

Claim 4

Dependent claim 4 recites:

> The method as recited in claim 1, wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature.

As described above, the combination of Bal and Yoshiura fails to teach the method as recited in claim 1. Specifically, the cited combination does not teach "associating a ***digital signature with a web page***," and "delivering the web page to

an electronic device capable of authenticating the ***digital signature*** and executing at least a portion of the web page after ***the digital signature*** is authenticated," as recited in claim 1. Furthermore, as noted previously, with respect to claim 3, there is no motivation provided in either reference that would suggest combining the teachings of Bal and Yoshiura. Accordingly, claim 4 is allowable over Bal in view of Yoshiura.

Claim 6 is not taught or suggested by the combination of Bal and Myer.

Claim 6

Dependent claim 6 recites:

> The method as recited in claim 1, wherein the web page is generated in an active server page (ASP) environment.

Myer describes a system that includes a master controller and one or more devices (e.g., a TV, a VCR, a CD changer, etc.) such that the master controller can be used to control the devices. As described above, Bal does not teach or suggest the features recited in claim 1. Specifically, Bal does not teach or suggest "associating a digital signature with a web page." Myer fails to add any teaching with respect to claim 1. Additionally, there is no motivation in either reference that would suggest combining the teachings of Bal and Myer. Therefore, and by virtue of its dependence on claim 1, claim 6 is allowable over Bal in view of Myer.

Claims 19, 32, and 34 are not taught or suggested by the combination of Bal and Renaud.

Claim 19

Dependent claim 19 recites:

> The system as recited in claim 17, wherein the confirmation module is included in the control object.

As described above, Bal does not disclose, teach, or suggest "a ***web page*** having a digital signature", as recited in claim 17, from which claim 19 depends. Rather, Bal discloses a ***control object*** having a digital signature, and examining a URL associated with a web page to determine whether or not the web page is authorized to invoke the control object. Bal does not disclose, teach, or suggest "a web page having a digital signature; an executable control object that may be invoked by [a] script in the web page; and a confirmation module configured to authenticate the digital signature to determine based on the authenticity of the digital signature, whether the control object should be invoked," as recited in independent claim 17.

Furthermore, Renaud discloses methods, apparatuses, and products that reduce the computational demands placed on both source user computer systems and receiving user computer systems by requiring the implementation and the verification of only a single digital signature for an arbitrary number of data files.

(Renaud, column 4, line 67 – column 5, line 4.) Renaud does not disclose, teach, or suggest a confirmation module included in a control object where the confirmation module is configured to authenticate a digital signature that is associated with a web page. Accordingly, the combination of Bal and Renaud does not teach or suggest the features of independent claim 17, from which claim 19 depends.

The Office cites Renaud column 4, lines 15-19 as disclosing "wherein the confirmation module is included in the control object," as recited in claim 19. The cited portion of Renaud states:

> "In another embodiment, computer-readable program code includes code for running the applet and code for determining whether the applet performs an action that triggers a security check. In another embodiment, code is included for use in establishing a secure connection with a remote site."

The cited text in no way teaches or suggests a confirmation module included in a control object, as claimed. Accordingly, and by virtue of its dependence on claim 17, claim 19 is therefore allowable over Bal in view of Renaud.

Claims 32 and 34

Independent claim 32 recites:

> A control object stored in a computer-readable medium, comprising computer-executable instructions that, when executed on a computer, perform the following:
>
> authenticating a web page that invokes the control object, wherein the authenticating is performed based on a digital signature associated with the web page; and
>
> executing a data-handling task on the computer if the web page is determined to be authentic.

Claim 32 recites "a digital signature associated with the web page." As discussed above with reference to claim 3, neither Bal nor Renaud disclose, teach, or suggest a web page having an associated digital signature, nor authenticating a web page based on a digital signature that is associated with the web page. Accordingly, claim 32 is allowable over Bal in view of Renaud.

Claim 34 is allowable by virtue of its dependence on claim 32.

Claims 27, 28, 30, and 31 are not taught or suggested by the combination of Bal and Liu.

Claims 27, 28, 30, and 31

Independent claim 27 recites:

> A web browser contained on a computer-readable medium of a client computer, comprising computer-executable instructions that, when executed by the client computer, perform the following:
>
> determining if a web page contains instructions to invoke a control object;
>
> determining if the web page has an associated digital signature;
>
> in an event that the web page has an associated digital signature, authenticating the web page using the digital signature; and
>
> invoking the control object if the source of the web page is authenticated.

Bal does not teach or suggest "determining if the web page has an associated digital signature," nor does Bal teach or suggest, "in an event that the web page has an associated digital signature, authenticating the web page using the digital signature." Liu does not add to the teaching of Bal regarding the cited claim features, nor does the Office claim that Liu adds to the teaching of Bal

regarding the cited claim features. Rather, the Office merely refers to Liu as teaching "determining if the web page contains instructions to invoke a control object." (*1/11/05 Office Action, p. 10.*) Accordingly, claim 27 is allowable over Bal in view of Liu.

Claims 28, 30, and 31 are allowable by virtue of their dependence on claim 27.

Conclusion

The Office's basis and supporting rationale for the §102 rejection of claims 1, 2, 5, 7-10, 17, 18, and 20-23 is not supported by the express teachings of Bal. The Office's basis and supporting rationale for the §103 rejections of claims 3, 4, 6, 19, 32, 34, 27, 28, 30, and 31 are not supported by the cited combinations of Bal, Yoshiura, Liu, Myer, and Renaud. Applicant respectfully requests that the §102 and §103 rejections be overturned and that pending claims 1-10, 17-23 27, 28, 30-32, and 34 be allowed to issue.

Respectfully Submitted,

Dated: 6/21/05 By: Kayla D. Brant

Kayla D. Brant
Reg. No. 46,576
(509) 324-9256 x 242

(9) Claim Appendix

1. method, comprising:

associating a digital signature with a web page; and

delivering the web page to an electronic device capable of authenticating the digital signature and executing at least a portion of the web page after the digital signature is authenticated.

2. The method as recited in claim 1, wherein the associating further comprises attaching the digital signature to the web page.

3. The method as recited in claim 1, further comprising:

determining if the web page includes code to invoke a control object; and

deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

4. The method as recited in claim 1, wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature.

5. The method as recited in claim 1, wherein the web page contains script that, when executed, invokes executable code that is executed on the electronic device executing the web page.

6. The method as recited in claim 1, wherein the web page is generated in an active server page (ASP) environment.

7. A method, comprising:

receiving a web page from a server, the web page containing executable script that, when executed, invokes a control object, the web page having a digital signature that can be used to identify a source of the web page;

determining whether the source of the web page is authentic via the digital signature; and

in an event that the source of the web page is authentic, displaying the web page and invoking the control object.

8. The method as recited in claim 7, further comprising:

in an event that the source of the web page is not authentic, refusing to invoke the control object.

9. The method as recited in claim 7, wherein the determining further comprises identifying the source of the web page.

10. The method as recited in claim 7, further comprising:

designating one or more authorized sources from which a web page that invokes a control object may be received; and

executing script contained in the web page only if the determining indicates that the web page was received from one of the one or more authorized sources.

17. A system, comprising:

a web browser configured to access a web page having a digital signature;

a processor configured to execute script contained in the web page;

an executable control object that may be invoked by the script in the web page and is executable on the processor; and

a confirmation module configured to authenticate the digital signature to determine based on authenticity of the digital signature, whether the control object should be invoked.

18. The system as recited in claim 17, wherein the confirmation module is called by the control object.

19. The system as recited in claim 17, wherein the confirmation module is included in the control object.

20. The system as recited in claim 17, wherein the confirmation module is included in the web browser.

21. The system as recited in claim 17, wherein the confirmation module is further configured to determine if the web page comes from a source that is authorized to invoke the control object and the control object is invoked only if the source of the web page is authorized to invoke the control object.

22. The system as recited in claim 17, wherein the confirmation module is called by the web page prior to the web page invoking the control object.

23. The system as recited in claim 17, wherein the digital signature module is not invoked if the web page does not have a digital signature.

27. A web browser contained on a computer-readable medium of a client computer, comprising computer-executable instructions that, when executed by the client computer, perform the following:

determining if a web page contains instructions to invoke a control object;

determining if the web page has an associated digital signature;

in an event that the web page has an associated digital signature, authenticating the web page using the digital signature; and

invoking the control object if the source of the web page is authenticated.

28. The web browser as recited in claim 27, further comprising:

determining if the web page contains executable script to invoke a control object; and

wherein the authenticating the web page further comprises authenticating the web page only if the web page contains executable script to invoke a control object.

30. The web browser as recited in claim 27, further comprising in an event that the web page does not have an associated digital signature, refusing to invoke the control object.

31. The web browser as recited in claim 27, further comprising instructions to determine if an authenticated web page comes from a source that is authorized to invoke the control object.

32. A control object stored in a computer-readable medium, comprising computer-executable instructions that, when executed on a computer, perform the following:

authenticating a web page that invokes the control object, wherein the authenticating is performed based on a digital signature associated with the web page; and

executing a data-handling task on the computer if the web page is determined to be authentic.

34. The control object as recited in claim 32, further comprising instructions to determine if a source of the web page is authorized to invoke the data-handling task prior to executing the data-handling task.